

PCPD



HK

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

社創及科技研討會2024

數據安全及AI應用

黎智敏女士
助理個人資料私隱專員
(企業傳訊及合規)

2024年12月11日



網絡安全風險與日俱增

PCPD



H K

全球趨勢

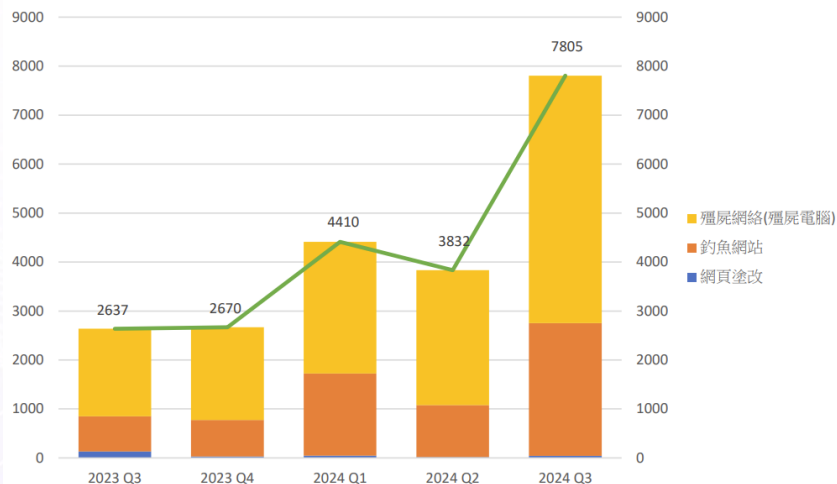
- 電訊公司Verizon的2023資料外洩調查報告顯示於**2013至2022年間**，資料外洩事故**大幅增加逾三倍**
- 市場調查公司Forrester 2023年的研究顯示**77%**的受訪機構表示於過去一年**曾遭受至少一次網絡攻擊**

本港趨勢

- 根據《香港保安觀察報告》¹，2024年第三季度涉及香港的網絡保安事件宗數比上季**上升104%**，比去年同季更**上升196%**
- **殭屍網絡**（佔整體案例64.7%）是本地網絡保安事故的主要原因；其次為**釣魚網站**（佔整體案例34.7%）

¹香港保安觀察報告 (2024年第三季度)：

[https://www.hkcert.org/f/report/912892/916161/2024Q3%20HK%20SecurityWatchReport%20\(Chinese\).pdf](https://www.hkcert.org/f/report/912892/916161/2024Q3%20HK%20SecurityWatchReport%20(Chinese).pdf)



海外資料外洩事故的例子

Medibank says hacker accessed data of 9.7 million customers, refuses to pay ransom

Reuters

November 8, 2022 5:05 AM GMT+8 · Updated a year ago



Casino giant MGM expects \$100 million hit from hack that led to data breach

Reuters

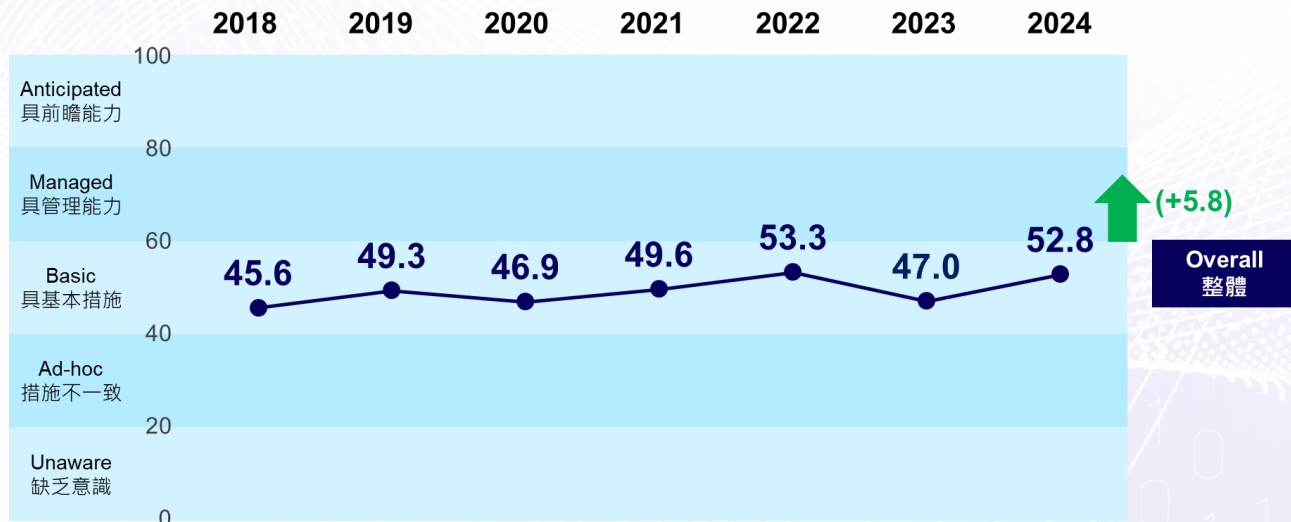
2 minute read · Published 9:40 PM EDT, Thu October 5, 2023



An exterior view of MGM Grand hotel and casino, after MGM Resorts shut down some computer systems due to a cyber attack in Las Vegas, Nevada, U.S., September 13, 2023. Bridger Bennett/Reuters

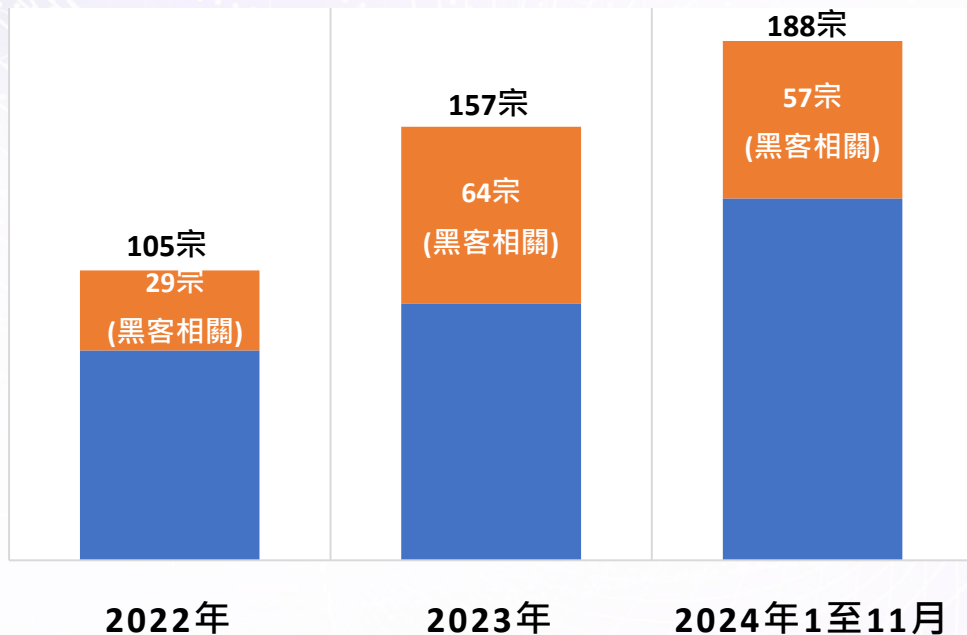
香港企業網絡保安準備指數

- 私隱專員公署及香港生產力促進局上月共同公布「香港企業網絡保安準備指數及AI安全風險」調查報告結果，「香港企業網絡保安準備指數」錄得**52.8點**（最高100點），較去年**上升5.8點**，重回接近2022年水平，但仍然維持於「具基本措施」級別，可見企業仍然有很大的進步空間
- 調查發現，**只有三分之一（35%）**的受訪企業**有為員工進行網絡安全意識培訓**，以及**只有四分之一（24%）**有**進行演習**以加強員工的網絡安全意識；顯示企業需於這兩方面加強



公署接獲的資料外洩事故通報

資料外洩事故通報



- 公署於2023年共接獲**157宗**資料外洩事故通報，比2022年的105宗**上升近五成**
- 而公署於**2024年首11個月**已接獲**188宗**通報，達2023年全年總宗數約**120%**
- 於2023年涉及**黑客入侵**的資料外洩事故共**64宗**（佔全年事故的41%），比2022年的29宗（佔全年事故的28%），**大幅增加逾一倍**
- 於**2024年首11個月**，涉及**黑客入侵**的資料外洩事故共**57宗**

香港《私隱條例》的相關規定

資料外洩事故可構成違反《私隱條例》附表1的保障資料第4原則

保障資料第4(1)原則

資料使用者須**採取所有切實可行的步驟**，確保由資料使用者持有的個人資料受保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響



保障資料第4(2)原則

如資料使用者聘用（不論是在香港或香港以外聘用）**資料處理者**，以代該資料使用者處理個人資料，該資料使用者須採取**合約規範方法**或其他方法，以防止轉移予該資料處理者作處理的個人資料被未獲准許或意外地被查閱、處理、刪除、喪失或使用



資料外洩的常見原因

主要技術風險



網絡釣魚



未修補保安漏洞



低強度密碼



過時的操作系統
和應用程式



植入惡意軟件

非牟利機構的勒索軟件攻擊個案 (1)

- 2024年，非牟利機構A向私隱專員公署作出資料外洩通報，表示其伺服器遭**勒索軟件攻擊及惡意加密**。有關的勒索軟件屬**Trigona的變種**，合共八台伺服器、一台數據儲存器及18台電腦遭受勒索軟件攻擊及加密。黑客曾要求機構支付贖金，為已被加密的檔案解鎖。
- 事件涉及**超過72,300名**會員的個人資料，當中包括姓名、香港身份證號碼、護照號碼、相片、出生日期、地址、電郵地址、電話號碼及緊急聯絡人的姓名及電話號碼。



調查結果發現六項缺失：

1. 伺服器被意外地**曝露於互聯網**
2. 資訊系統欠缺有效的**偵測措施**
3. 沒有為管理員帳戶啟用**多重認證**功能
4. 欠缺資訊**保安政策**及指引
5. 沒有定期進行**風險評估**及**保安審計**
6. 欠缺離線**數據備份**方案



非牟利機構的勒索軟件攻擊個案 (2)

- 2022年，私隱專員公署收到一間學會的資料外洩事故通報，指其名下六台載有個人資料的伺服器遭**勒索軟件攻擊及惡意加密**。
- 事件影響**超過13,000名會員及約10萬名非會員**的個人資料，除了姓名、聯絡資料、僱主名稱及職位外，部份人士的身份證號碼、信用卡號碼（不包括卡驗證碼）、出生日期、專業認證詳情及考試結果亦受影響。



調查結果發現**三項缺失**：

1. 資料保安**風險管理**欠佳
2. 資訊**系統管理**有欠妥善
3. 未適時啟用**多重認證功能**



資訊及通訊科技的保安措施

資料保安建議措施

七大建議措施一覽

- 1 資料管治和機構性措施
- 2 風險評估
- 3 技術上及操作上的保安措施
- 4 資料處理者的管理
- 5 資料保安事故發生後的補救措施
- 6 監察、評估及改善
- 7 其他考慮

下載指引



下載小冊子



資料保安建議措施

技術上及操作上的保安措施

資料使用者應採取**足夠及有效的保安措施**，以保護其控制或所持有的個人資料和資訊及通訊系統：



保護電腦網絡



資料庫管理



存取管控



防火牆和
反惡意軟件



保護網絡應用程式



加密



電郵及檔案傳送



資料備份、銷毀
及匿名化

資料保安建議措施

技術上及操作上的保安措施

資料使用者應採取**足夠及有效的保安措施**，以保護其控制或所持有的個人資料和資訊及通訊系統：



保護電腦網絡



資料



保護網絡應用程式

- 在網絡安裝**防火牆**，以防止未經許可的網絡連接，亦可偵測網絡攻擊
- 在電腦及伺服器安裝**防毒軟件**（反惡意軟件），以偵測及防止病毒及威脅
- 定期進行**保安漏洞評估**及**滲透測試**
- 使用**網站安全掃描服務**，定期掃描以偵測最新的已知或潛在的網絡安全風險
- 及時更新正在使用的系統及軟件，可以**修補保安漏洞**，減少被攻擊的機會

資料保安建議措施

資料保安事故發生後的補救措施

資料使用者在資料保安事故發生時可採取的補救措施：

停止並中斷連接
受影響的系統



更改密碼或
中止權限



更改系統配置



通知受影響人士
並提供建議



通知私隱公署
及其他執法或監管
機構



修補保安漏洞



在可行情況下
掃描系統



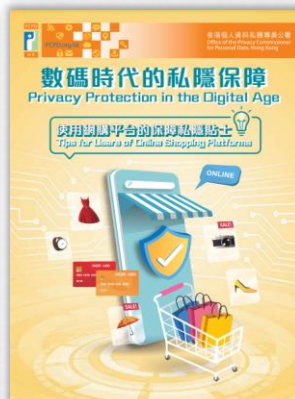
汲取經驗及教訓



NOTE

資料使用者亦應從資料保安事故中汲取經驗及教訓，覆檢和加強其整體資料管治和資料保安措施

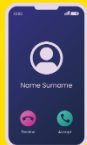
資訊科技相關指引及報告



www.pcpd.org.hk



「數據安全」套餐 “Data Security” Package



數據安全熱線
Data Security Hotline
2110 1155



數據安全快測
Data Security Scanner
<https://www.pcpd.org.hk/Toolkit/tc/>



數據安全專題網頁
Data Security Webpage
https://www.pcpd.org.hk/tc_chi/data_security/index.html



免費名額參加研習班及講座
Free quotas to join professional
workshop and seminars



PCPD



H K



[PCPD.org.hk](https://www.pcpd.org.hk)

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong







AI應用



AI的私隱風險



風險	闡釋	例子
資料外洩 	AI系統（如聊天機械人）可能會保留大量的用戶紀錄，使其成為黑客的目標，導致潛在的資料外洩。	2023年3月，ChatGPT發生重大資料外洩事故，洩露了用戶的對話標題、姓名、電子郵件地址以及信用卡號的後四位數字。
資料使用 	AI模型非常先進，以至於人們難以理解他們的個人資料將如何被使用。	一些AI模型可以識別某些患者的種族，即使這不是模型的原有目的。
過度收集資料 	AI應用程式傾向收集和保留越多的數據，包括個人資料。	據報導，OpenAI在網上擷取了3,000億個單字來訓練ChatGPT。
資料準確性 	訓練AI模型需要大量數據。但當數據的品質和準確性參差時，AI系統就有可能提供錯誤的分析。	一家跨國公司的AI招聘系統使用有偏見的數據進行訓練，分析結果較偏向男性申請人。

深度偽造 (Deepfake)

製作詐騙影片

AI偽造高層 出席視像會議 指令匯款呢走跨國公司 兩億



拆解\$3.6億
「後生仔詐騙集團」招式
警演示
用Deepfake男扮女
中英手冊逐字逐句教扮慘
業績龍虎榜鼓勵呢多啲

偽冒官員及名人

【騙局大拆解】

點樣可以分辨片段真偽?

假

假

假

假

AI扮政府官員再叫你投資? 一不留神就會中招!

利用深偽技術進行的網上投資騙案

EVERYONE CAN BECOME A PARTNER! THE LAW WAS SIGNED

EVERYONE CAN BECOME A PARTNER! THE LAW WAS SIGNED



START INVESTING WITH JUST HK\$2000 AND WITHDRAW HK\$60000 EVERY WEEK!

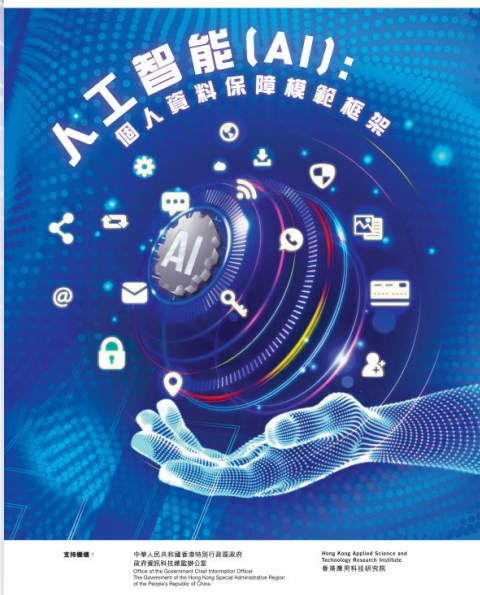
START INVESTING WITH JUST HK\$2000 AND WITHDRAW HK\$60000 EVERY WEEK!

《人工智能 (AI) : 個人資料保障模範框架》

PCPD



HK



亮點



體現國家的《全球人工智能治理倡議》



人工智能安全乃國家安全重點領域之一



為有意採購、實施及使用AI，包括生成式AI的機構提供國際認可及切實可行的**建議和最佳行事常規**

好處



協助機構遵從《個人資料(私隱)條例》的相關規定



促進AI 在香港**健康發展**

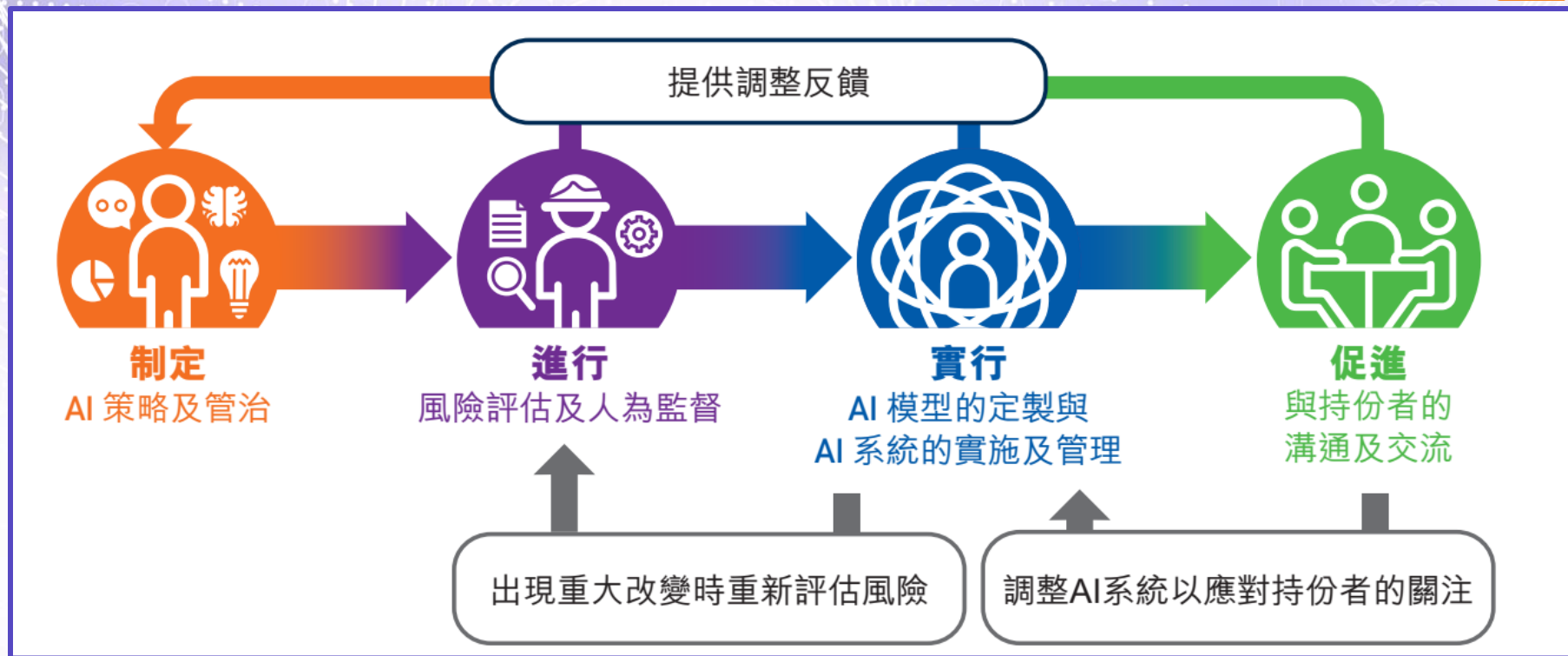


促進香港成為**創新科技樞紐**



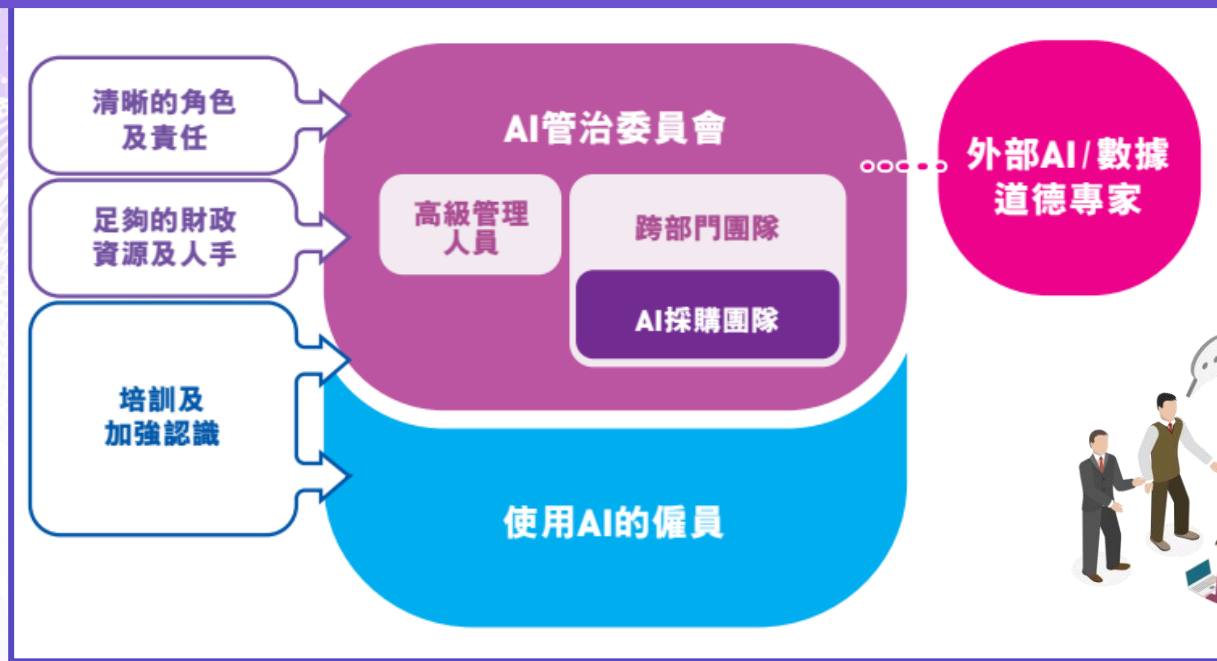
推動香港以至大灣區的**數字經濟發展**

《人工智能 (AI)：個人資料保障模範框架》



管治架構

機構應建立具足夠資源、專業知識和決策權的內部管治架構，以引領 AI 策略的實施，並監督 AI 系統的採購、實施及使用



進行風險評估及人為監督

- 在採取風險為本的方式時，所採取的緩減風險措施的類別和程度應與已識別的風險程度相符和相稱

若使用 AI 系統產生的輸出結果在某些情況下很可能對個人造成嚴重及長期的損害，且該風險無法充分減低，有關 AI 系統應被視為高風險。

較低

AI 系統的風險程度

較高



人在環外

AI 在沒有人為介入下作出決定



人為管控

人類決策者監督 AI 的運作，在有需要時介入



人在環中

人類決策者在決策過程中保留控制權以防止及/或減低 AI 出錯

可能帶來較高風險的AI應用例子



AI 輔助醫學
影像分析或治療



使用生物識辨資料
實時識別個人



求職者評估、工作表現評核
或終止僱傭合約



評估個人享用社會福利或
公共服務的資格

AI模型的定製與AI系統的實施及管理

主要流程



準備及管理數據



定製及實施



管理及持續監察

部分建議



- 遵循《私隱條例》的規定
- 盡量減少定製及使用AI所涉及的個人資料
- 管理用以定製及使用AI模型的數據
- 妥善記錄處理數據的情況

- 進行嚴格測試及驗證，並在使用前評估其可靠性、穩健性和公平性
- 視乎機構如何將 AI 方案整合（即在機構的本地內部伺服器或由第三方提供的雲端伺服器運行），機構或需考慮其他因素，以符合《私隱條例》的規定
- 確保系統安全及數據安全

- 妥善地記錄存檔
- 定期對 AI 系統進行內部審核
- 制定 AI 事故應變計劃
- 考慮採取檢視機制



促進與持份者的溝通及交流



與持份者的溝通



披露AI系統的
使用



提供充足資訊



披露風險



與持份者的交流



容許拒絕使用
AI及資料查閱
和改正



按要求提供
解釋



提供人為介入
的選擇



聯絡我們

 查詢 2827 2827  傳真 2877 7026

 網址 www.pcpd.org.hk

 電郵 communications@pcpd.org.hk

 地址 香港皇后大道東248號大新金融中心13樓1303室



保障、尊重個人資料私隱

Protect, Respect Personal Data Privacy

追蹤我們
最新資訊



PCPD



H K

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

謝謝！

Thank you!

